



QUALYS SECURITY CONFERENCE 2020

Building an Always Up-to-Date, Real-Time View of Your Global IT Assets in the Hybrid IT Environment

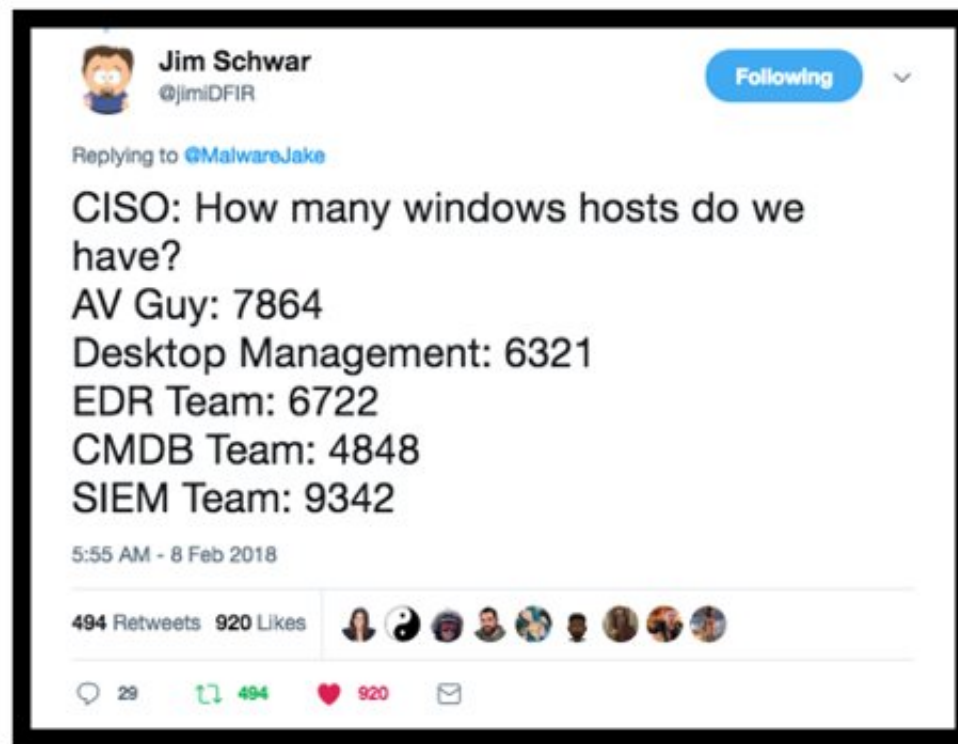
Chris Carlson
VP, Product Management, Qualys, Inc.

Starting Point...

Knowing what's on your
Global Hybrid IT
environment is
fundamental to security



Not an Easy Problem to Solve



Cloud
Agent



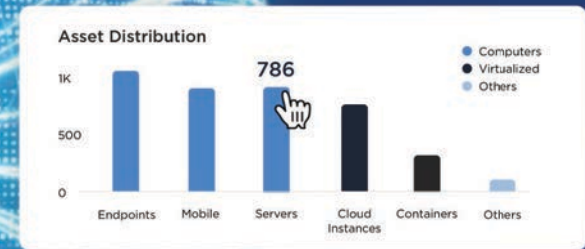
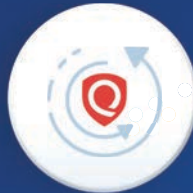
Passive
Sensor



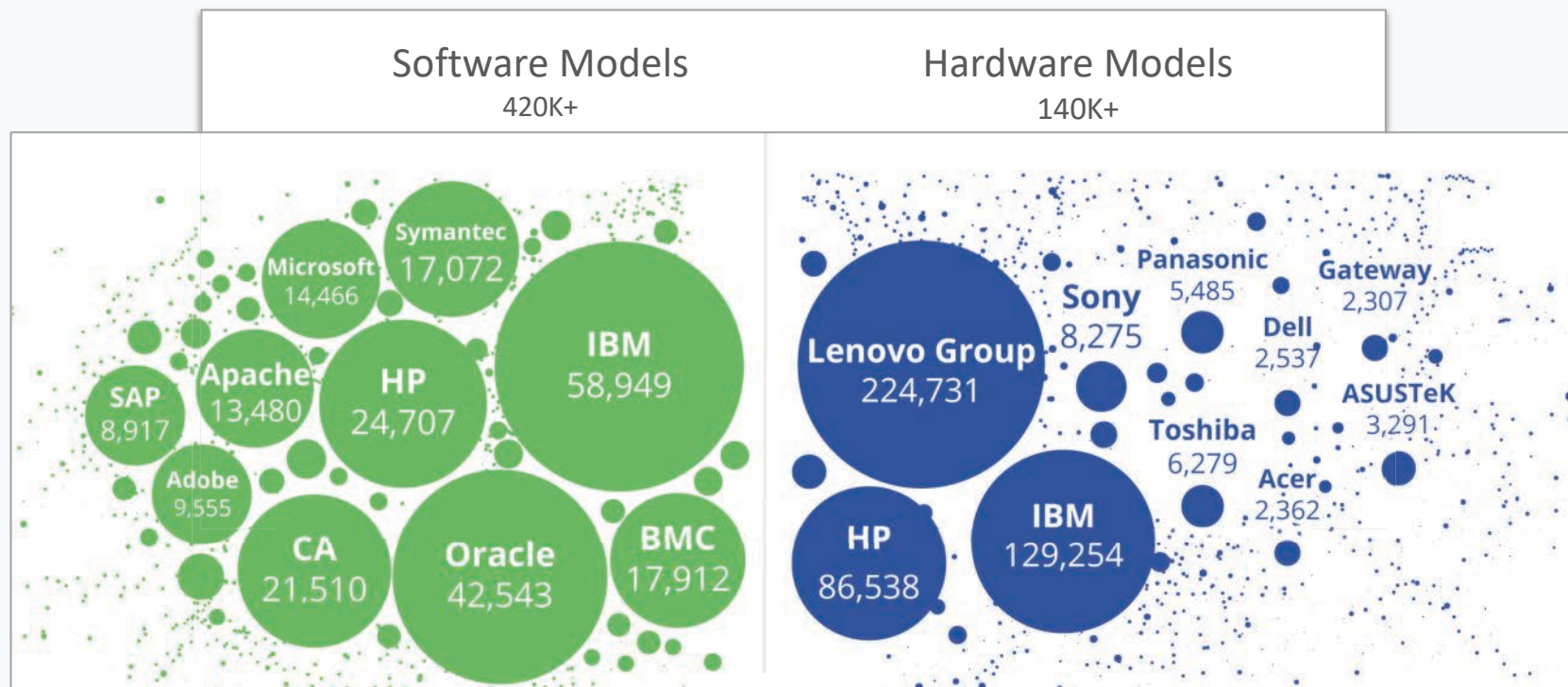
Network
Scanner



Cloud
Connectors



Asset Inventory Catalog



Hardware

Operating System

Software

Raw Data	Dell R510	Base OS Runtime AIX: 06.01.0009.0300 EE	mysql-community-server 5.6.35-2.el7.x86_64
----------	-----------	--	---

Vulnerabilities BETA

52.1K

Total Detections

SEVERITY

4	25.6K
5	15.0K
3	9.78K
2	1.53K
1	221

CATEGORY

Windows	29.8K
Local	9.46K
Internet Explorer	8.31K
Office Application	1.28K
Security Policy	956
SUSE	741
CentOS	712
Fedora	314
Web server	154

Asset ▾



operatingSystem.category:Server and software:(category:Database)



Asset

Vulnerability

Group By: Vulnerability ▾



Filters ▾

1 - 50 of 4365



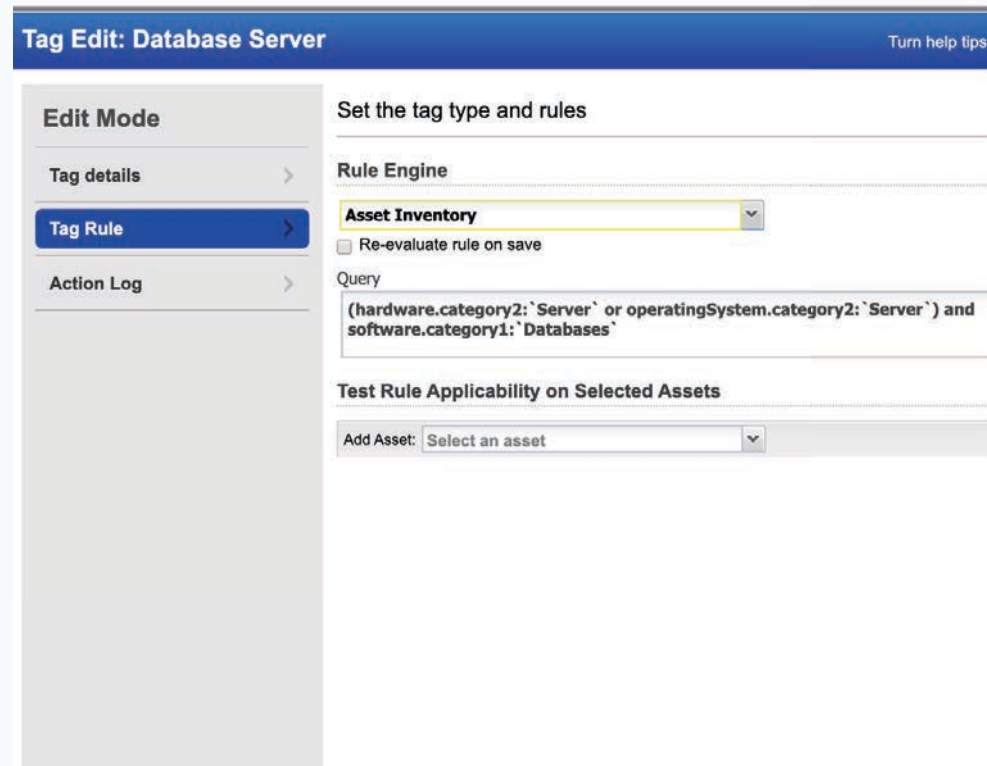
QID	TITLE	CVE IDS	SEVERITY	VULNERABILITY COUNT
91495	Microsoft Windows Security Update January 2019	CVE-2019-0571 CVE-2019-0570 24 more...	<div><div></div><div></div><div></div><div></div><div></div></div>	109
91504	Microsoft Windows Security Update February 2019	CVE-2019-0595 CVE-2019-0597 30 more...	<div><div></div><div></div><div></div><div></div><div></div></div>	109
91488	Microsoft Windows Security Update December 2018	CVE-2018-8649 CVE-2018-8638 14 more...	<div><div></div><div></div><div></div><div></div><div></div></div>	107
91481	Microsoft Windows Security Update November 2018	CVE-2018-8407 CVE-2018-8408 21 more...	<div><div></div><div></div><div></div><div></div><div></div></div>	107
91470	Microsoft Windows FragmentSmack Denial of Service Vuln...	CVE-2018-5391	<div><div></div><div></div><div></div><div></div><div></div></div>	105
100131	Microsoft Internet Explorer Mouse Tracking Events Design ...	—	<div><div></div><div></div><div></div><div></div><div></div></div>	105

Auto-Tagging using Catalog Attributes

Asset Inventory catalog attributes are extended to the tagging rule engine

Auto-Tagging rules uses QQL syntax (no groovy!)

Use catalog auto-tags to solve the “OR” reporting problem



The screenshot displays the 'Tag Edit: Database Server' interface. On the left, a sidebar under 'Edit Mode' contains links for 'Tag details', 'Tag Rule' (which is selected and highlighted in blue), and 'Action Log'. The main content area is titled 'Set the tag type and rules'. It includes a 'Rule Engine' section with a dropdown menu set to 'Asset Inventory' and a checkbox for 'Re-evaluate rule on save'. Below this is a 'Query' field containing the QQL: `(hardware.category2: `Server` or operatingSystem.category2: `Server`) and software.category1: `Databases``. At the bottom, there is a section 'Test Rule Applicability on Selected Assets' with an 'Add Asset' dropdown menu currently showing 'Select an asset'.

Eliminate Asset Blind Spots for your Security Program

Passive Sensor (included in VMDR) discovers assets in real time and provides context of how these devices communicate

Immediate visibility of unknown unmanaged devices between VM scan windows

VMDR adds new workflows

- auto-tag unmanaged assets
- activate for VM scanning
- trigger 3rd party install of Cloud Agent



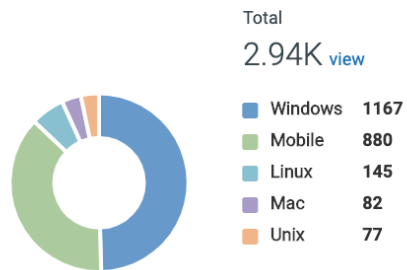
Unmanaged Assets ▾



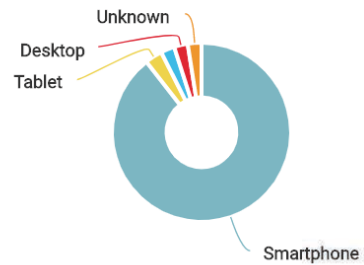
Last 30 Days ▾



UNMANAGED (PASSIVE SCANNING)



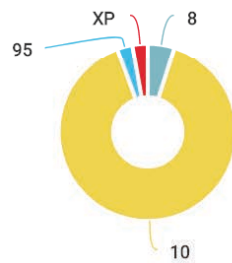
UNMANAGED ASSET CATEGORY



NEW DISCOVERIES IN LAST 4 HOURS

1

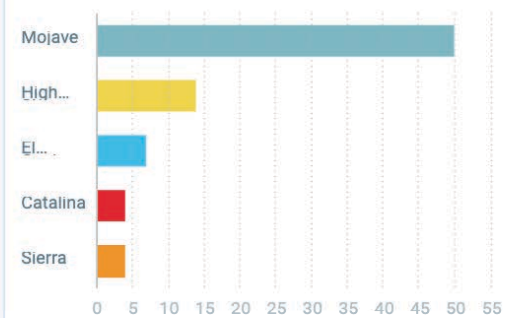
WINDOWS OS

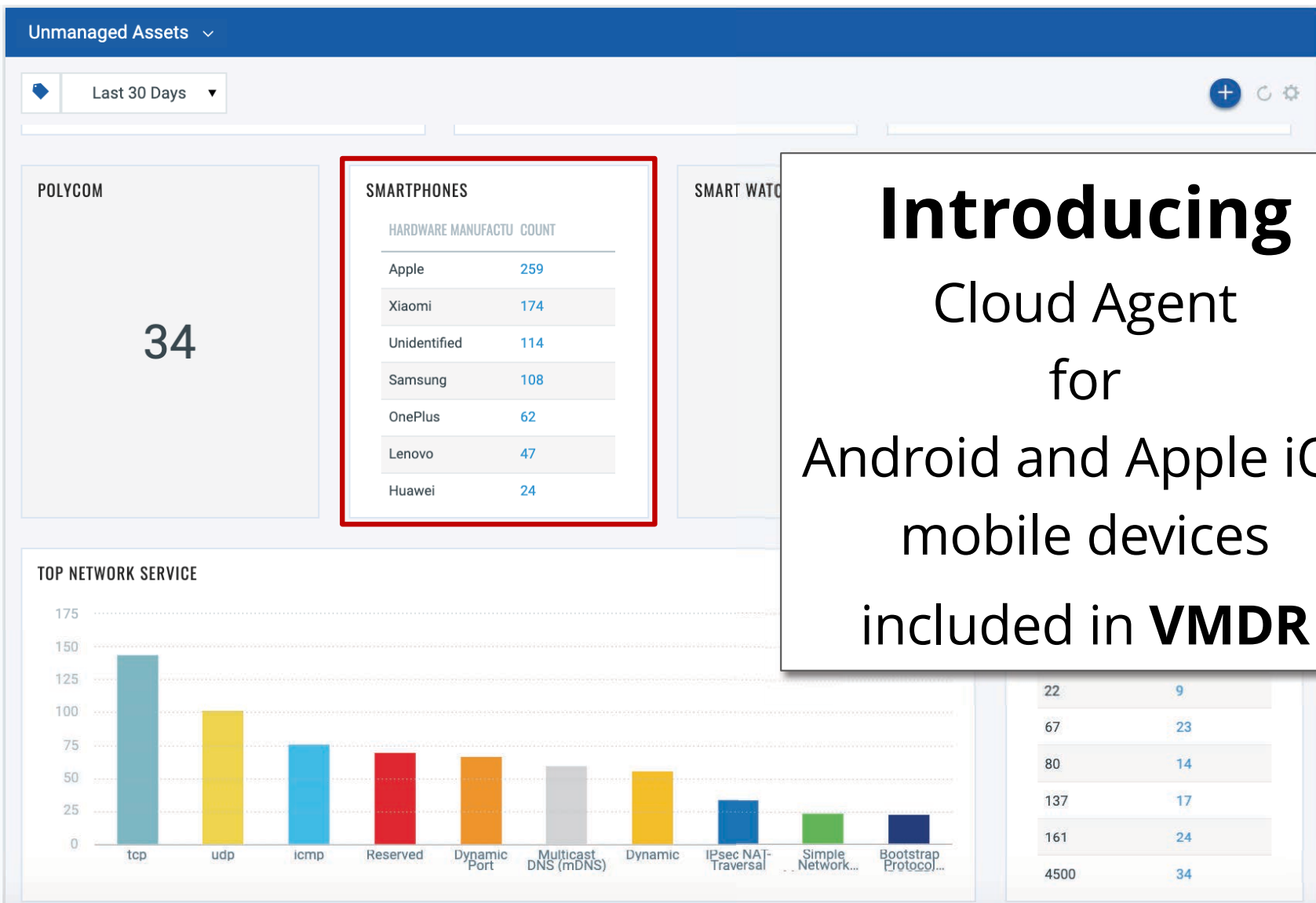


USERS WITH UNMANAGED ASSETS

ACCOUNT USERS	COUNT
spabbuleti/CORP	2
spabbuleti/CORP.QUALYS.COM	2
adhumale/CORP	1
adhumale/CORP.QUALYS.COM	1
adhumale/corp.qualys.com	1
dgao/CORP	1
dgao/CORP.QUALYS.COM	1

MAC OS





Introducing
Cloud Agent
for
Android and Apple iOS
mobile devices
included in **VMDR**

A small, dark blue rounded square icon containing the white text "AI".

AI

DEMO

Asset Inventory

Software Normalization + Catalog
VM Dashboard and Searching



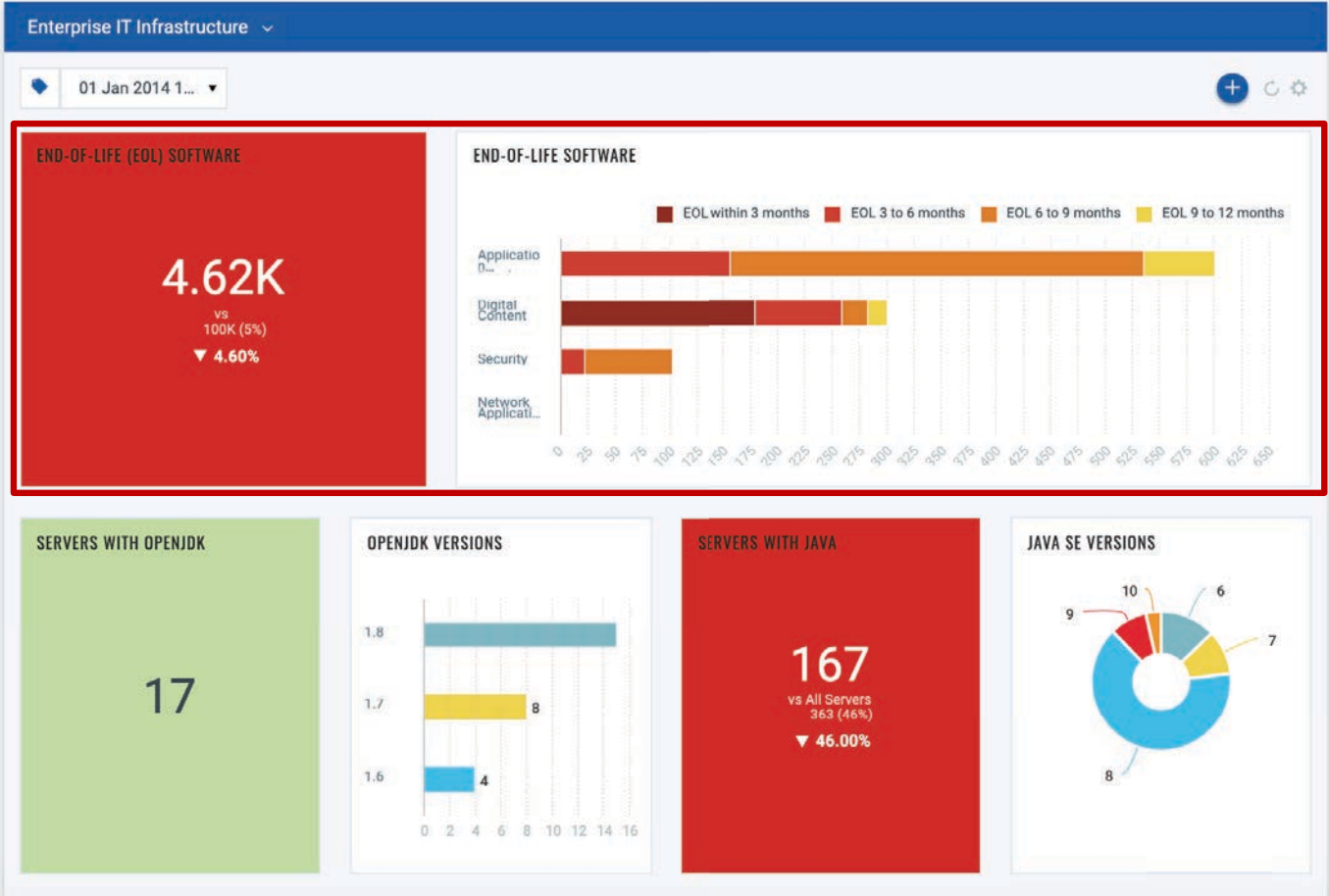
Enhance VMDR
with additional
Asset Inventory
add-on capabilities

Hardware and Software Lifecycle (EOL/EOS)

Current and Future
EOL and EOS

Make remediation
decisions based on
current and future
EOL status

Sunset vs. Patching



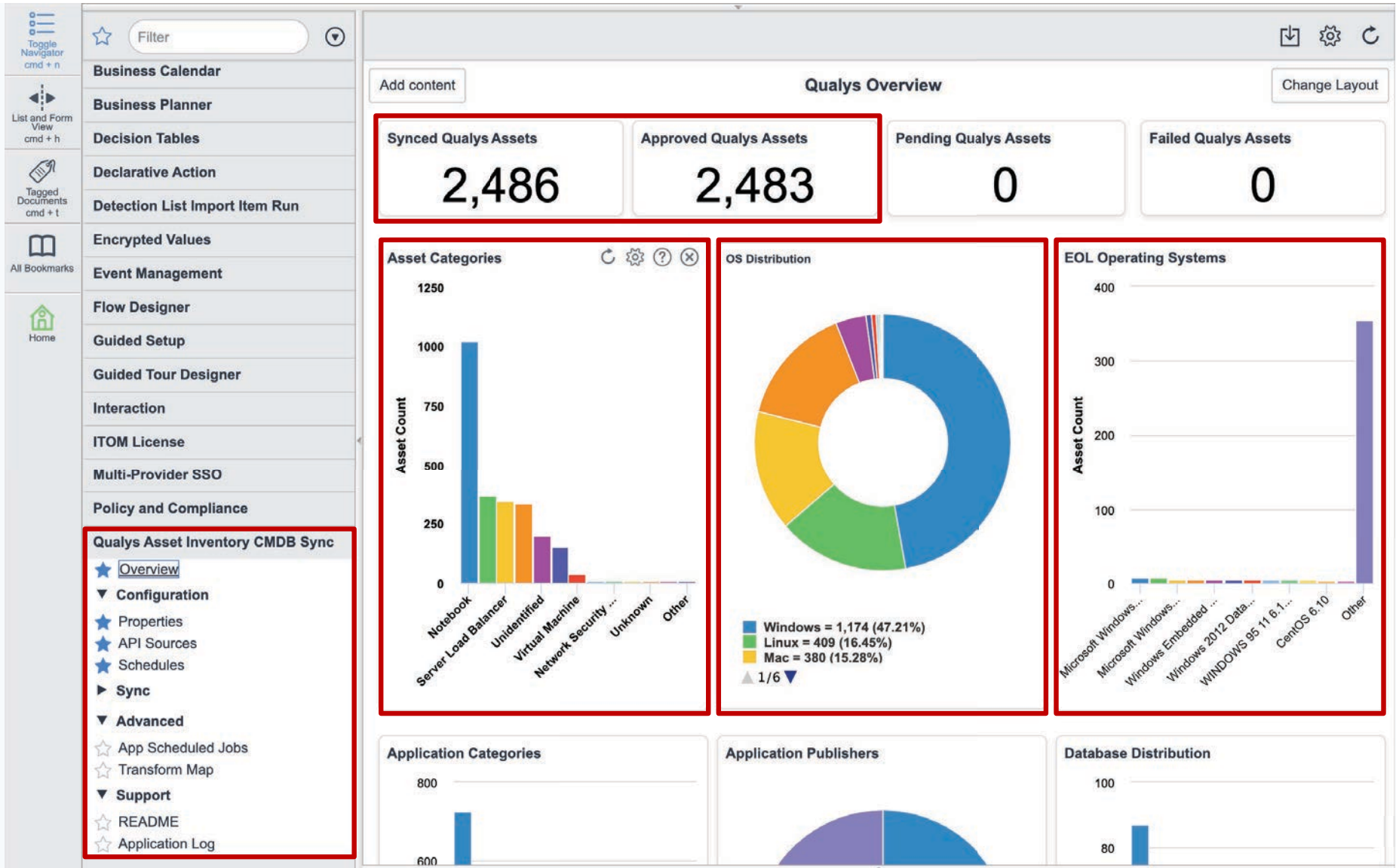
Asset Inventory CMDB Sync

Use Qualys VMDR sensors for asset discovery (scanner, agent, cloud, container, mobile device, more)

Continuous sync for enriched asset data into ServiceNow CMDB (certified for 3 last releases)

Assets are automatically mapped to Configuration Item (CI) Classes





New: Software Usage for Patching... or Uninstall

Installed Software

Search Last 30 days

5 5 1 1

Dropbox

Type: Application
Category: Storage / Backup and...
License Category: Commercial

Publisher: Dropbox
Product: Dropbox
Edition: -

Market Version: 84
Version: 84.4
Update: 84.4.170

Architecture: 64-bit
Component: -
Language: English

Install Path: C:/Program Files...
Install Date: Jan 20, 2019
Last Use Date: Nov 10, 2019

Lifecycle Stage: EOL (Extended Support)

GA: Oct 30, 2019
EOL (Estimated): Nov 14, 2019
EOS (Estimated): Nov 14, 2019

1 - 50 of 79

	RELEASE	INSTALLED ON
Agent	3.1.0.101	-
Internet Explorer	11.0.14393.2007	Jan 15, 2018
Dropbox	84.4.170	Jan 20, 2019
Help	1.2.3	Jun 7, 2018
Core	5.6.7	Oct 19, 2018
Version of Microsoft XML (MSXML) v3 :	8.110.14393.2906	Jan 15, 2018
Windows Defender File ProgramFiles%\Windows Defender\MpSvc.dll) Version:	4.10.14393.2999	Jan 15, 2018

Summary and Take-Aways

Great Security Programs start with Great Asset Inventory

Use the included Qualys VMDR sensors for asset discovery across all asset types for your hybrid IT environment

Always up-to-date normalized view with catalog attributes gives asset context to VM programs

Enhance VMDR with additional Asset Inventory capabilities: EOL/EOS Lifecycle, CMDB Sync, Software Usage



QUALYS SECURITY CONFERENCE 2020

Thank You

Chris Carlson
ccarlson@qualys.com